IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,	)	
Plaintiffs,	)	Civil Action No. 96-1285
	)	(Judge Lamberth)
v.	)	
GALE A. NORTON, et al.,	)	
Defendants.	)	

DEFENDANTS' RESPONSE TO PLAINTIFFS' NOTICE OF SUPPLEMENTAL INFORMATION IN SUPPORT OF PLAINTIFFS' MOTION FOR INFORMATION TECHNOLOGY SECURITY PRELIMINARY INJUNCTION

On October 3, 2005, Plaintiffs filed a "Notice of Supplemental Information" in support of their pending motion for a preliminary injunction (the "Notice"). The Notice, however, contains no information that is not already before the Court, either from the 59-day hearing or through the documents filed by the Defendants on September 28, 2005.[1] Instead, the Notice, through the guise of "supplemental information," serves as nothing more than an inappropriate vehicle for baseless arguments and a scurrilous attack on Defendants' closing argument and the record evidence that supports it.

Plaintiffs were afforded the opportunity to rebut Defendants' closing argument at the conclusion of the evidentiary hearing. Without justification, Plaintiffs now seek to supplement

[1] To the extent that the Notice recites any information not presented during the evidentiary hearing, it simply reiterates information that Defendants made available to the Court on September 28, 2005, by filing a September 6, 2005 memorandum from the Inspector General ("IG") for the Department of the Interior ("DOI") and two September, 2005 reports concerning penetration testing related to the National Business Center ("NBC") prepared by Internet Security Systems ("ISS").

their rebuttal some two months after the hearing closed and the matter was submitted. Further, Plaintiffs' allegations regarding the basis for statements made in Defendants' closing argument simply ignore the record support for that argument. The record fully supports every argument addressed in the Notice and the strength of this support is not diminished by Plaintiffs' overheated and unsupported rhetoric. Accordingly, Plaintiffs' Notice should be summarily rejected.

I. Defendants Have Not Withheld Or Concealed Material Information From The Court Or Plaintiffs

Without foundation, Plaintiffs assert that Defendants' September 28 filing "confesses" that "trustee-delegates and their counsel had knowledge of materially adverse information, but concealed it from this Court and plaintiffs during the preliminary injunction hearing... ." Notice at 2. This assertion is groundless, as there is no "confession," no knowledge of materially adverse information prior to the closing argument, and no concealment. Nothing in Defendants' September 28 filing, consisting of material prepared for and by the Office of the Inspector General, constitutes a confession by the Department of the Interior or "materially adverse information" known to Defendants prior to the conclusion of the evidentiary hearing on July 29, 2005.

Plaintiffs' contention that, during the hearing, Defendants concealed the information contained in the IG's September 6, 2005 report and the two September, 2005 reports related to NBC defies temporal reality. The IT security hearing concluded on July 29, 2005. The three reports included in the September 28 filing were not even in existence on July 29, and were not issued until September, 2005, well after the close of the hearing. There is no way that Defendants, or anyone else, could have concealed or withheld documents that did not exist.

Moreover, both the September 2005 technical report and the September 2005 management report concerning the external penetration test state that the testing occurred from July 6, 2005 through approximately July 29, 2005, and that the test results were not documented or validated by ISS until September 6, 2005. September 2005 Technical Report, p. 6; September 2005 Management Report, p. 4. Similarly, the cover pages prepared by ISS for both the technical report and the management report indicate that the testing was conducted in July and August, 2005. Thus, there is no way that Defendants could have concealed this information from anyone during the hearing. Similarly, no basis exists to argue that Defendants' counsel possessed knowledge of the testing prior to the conclusion of the IT security hearing. The penetration tests conducted by ISS on behalf of the Office of the Inspector General were performed in a "blind" mode, and ISS communicated only with the primary contact at the OIG, with no one at the National Park Service or NBC being informed of the testing activity. September 2005 Management Report, p. 6. In short, the targeted agencies (and Defendants' counsel) were unaware of the tests by design. At the end of their Notice, Plaintiffs tack on rambling assertions in an apparent attempt to bolster their unfounded claim that Defendants somehow concealed information during the hearing. They state:

> There is no doubt that the material adverse information disclosed in the Notice [Defendants' September 28 filing] - nearly two months after the conclusion of the evidentiary hearing - was known to Gillett and the trustee-delegates during the evidentiary hearing inasmuch as the[y] were in possession of at least the **July 13, 2005 ISS report** regarding the penetration of NBC for at least two weeks during the hearing. Instead of candor, they again chose to conceal this report . . . in willful violation of the April 25, 2005 Court order.

Notice at 8-9 (emphasis in original). These allegations are false and are refuted by the record.

Defendants did not conceal the July 13, 2005 ISS report regarding the initial penetration of NBC.[2] To the contrary, Defendants produced that report to Plaintiffs on July 26, 2005, Exh. 1, and Plaintiffs introduced it into evidence at the hearing the next day, as Plaintiffs' Exhibit ("PX") 651. On top of that, Plaintiffs questioned Hord Tipton, Chief Information Officer, Department of the Interior, at length about the contents of the report. Exh. 2 (Tr., Day 57 PM, pp. 22-38). Far from being concealed, the July 13, 2005 ISS report on the penetration testing of NBC is part of the hearing record and was discussed in court.[3]

---

[2] Evidence concerning the earlier ISS penetration of NBC was the subject of extensive testimony by Mr. Philip Brass between May 6 and May 9, 2005. Thus, even before the July 13 report was issued, Plaintiffs had full opportunity to examine its principal author. To the extent that there was "material adverse information" developed by Mr. Brass about the NBC systems, Plaintiffs were aware of it from the earliest days of the IT security hearing.

Plaintiffs were also aware of the differing views of the NBC test results from the earliest days of the IT security hearing. Ms. Mary Kendall, the OIG's Deputy Inspector General and General Counsel, was questioned about a memorandum to the Inspector General from P. Lynn Scarlett, Assistant Secretary for Policy, Management and Budget, concerning the results of the ISS penetration test on the NBC IT systems. PX 33. Ms. Kendall was also questioned about the response of the OIG to Ms. Scarlett. PX 34. See Exh 3 (Tr., Day 7 AM, pp. 41-59; Tr., Day 7 PM, pp. 5-15).

[3] In citing the July 13, 2005 ISS report in his September 6, 2005 memorandum, the IG added the full date of the report to its title: " NSM-EV-OSS-0025-2005-7-13-05-NBC Penetration Testing External Penetration Testing of National Business Center. July 13, 2005." September 6, 2005 Memorandum, p. 4, n.6. Earlier, in the July 13, 2005 memorandum from Mike Wood, the July 13, 2005 ISS report was identified as "OIG Report NSM-EV-OSS-0025-2005 NBC Penetration Testing External Penetration Testing of National Business Center," without the full date of the report listed in the title. PX651, p. 1. Giving Plaintiffs the benefit of the doubt, they may have been confused by the slight difference between the two references. Notice, p. 9 fn. 8. Nevertheless, Defendants clearly provided the July 13, 2005 ISS report concerning the external penetration testing of NBC to both the Court and Plaintiffs and Plaintiffs admitted it into evidence. Obviously, nothing was concealed.

The July 13, 2005 ISS report addresses penetration testing of NBC that is entirely separate from the additional penetration testing of NBC that was reported upon in the submitted September, 2005 ISS reports. As Plaintiffs' Exhibit 651 makes clear, ISS was, in that document, reporting on penetration testing that took place from March, 2005 through April 15, 2005. PX651, pp. 1, 7. In contrast, the September 2005 ISS report submitted with Defendants' September 28 filing addresses penetration testing that took place during a completely different period - from July 6, 2005, through approximately July 29, 2005. Therefore, contrary to Plaintiffs' assertion, the July 13, 2005 ISS report did not address the penetration testing about which the Court has been informed as a result of Defendants' September 28 filing.

The record, therefore, conclusively rebuts Plaintiffs' malicious allegation that "[t]here is no doubt that the material adverse information disclosed in the [September 28 filing] . . . was known to Gillett and the trustee-delegates during the evidentiary hearing . . . ." Notice at 8. Accordingly, Plaintiffs' allegation of concealment should be summarily rejected as without any factual or logical basis.

II. The Hearing Record Establishes That NBC Has Intrusion Detection Systems

Plaintiffs claim that Defendants falsely asserted in closing argument that Intrusion Detection Systems ("IDS") exist on the NBC IT system. Plaintiffs are wrong. Not only have the Defendants not admitted, "grudgingly"[4] or otherwise, in the September 28 Notice or elsewhere, that the NBC IT systems does not have IDS, Defendants cannot make such an admission because it is not true and the record demonstrates that the NBC IT systems do have IDS.

[4] Plaintiffs' Notice states that Defendant "grudgingly admits . . . that NBC has **no** intrusion detection systems." Notice at 3.

Although Plaintiffs assert that the September 28 filing contains an admission, Defendants certainly made - and make - no such admission, nor does any document filed by Defendant support this assertion. The hearing record contains unrefuted testimony and evidence that supports Defendants' assertion that NBC has IDS for its IT systems. Plaintiffs simply ignore this record evidence. For example, as correctly pointed out in response to a question from the Court during closing argument, Defendants' Exhibit 48 indicates that an IDS application was in place for NBC's DC-LAN General Support System.[5] Robert Haycock, NBC's Chief Information Officer ("CIO"), testified to his understanding that this intrusion detection device was in place. Exh. 6 (Tr., Day 49 PM, pp. 11-13). Notably, Mr. Haycock testified unequivocally that there are operational IDS in the NBC system. Exh. 10 (Tr., Day 48 PM, p. 86).

Consistent with Mr. Haycock's testimony, Kevin McWhinney, NBC's Chief of Enterprise Infrastructure Division, Denver, also testified in detail about the use of IDS at the

---

[5] Plaintiffs made a rebuttal argument at closing and addressed the IDS issue. Exh. 4 (Tr., Day 59 PM, p. 78). It is certainly irregular to permit additional rebuttal argument based upon events and information not available at the time the case was submitted.

If any basis exists for asserting that counsel made misrepresentations or misleading comments, it relates to Plaintiffs' closing argument. The evidence fails to support Plaintiffs' counsel's statements that NBC does not have any IDS devices. See Exh. 4 (Tr., Day 59 PM, p. 31, p. 32). Mr. Brass did not testify that there were not IDS devices on the NBC IT systems; the ISS NBC reports do not contain that assertion and there is no evidence to support that assertion. Plaintiffs' counsel questioned Mr. Brass very closely about the issue of whether there were "limited or no tools for monitoring, detection or prevention" on NBC systems, quoting from PX 19. Exh.5 (Tr., Day 5, pp. 61-62). In fact, Mr. Brass stated:

> And also I think the executive summary is sort of broader than I'm usually fond of stating things. You know, limited or no fools [sic] for monitoring, detection and prevention. You know, that's not a statement I usually make.

Exh. 5 (Tr., Day 5, p. 73).

NBC Denver Data Center. He testified without contradiction that:

> We have the firewalls and network intrusion detection sensors that are within key locations within the NBC Denver data center environment. Those devices are signature-based devices, meaning that if they determine the signature of some type of a network exploit, they will report that to a console, and we have it configured at this point within the data center so that they will also issue a command to the network device at the edge of the network to prevent any more traffic inbound from the source address.

Exh. 7 (Tr., Day 52 PM, pp. 33-34) (emphasis added). Mr. McWhinney graphically displayed this system, including the presence of "NIDS," in Defendants' Exhibit 60, which was displayed in the courtroom, for the Court's convenience. Exh. 7 (Tr., Day 52 PM, pp. 41, 51-52). Mr. McWhinney further testified that the NBC Denver data center uses a security information management product, NetForensics, that "captures log information that are indicative of potential, either anomalies or invalid access permissions from a variety of devices, including networks, firewalls, network intrusion detection sensors primarily, at this point in time." Exh. 7 (Tr., Day 52 PM, p. 35) (emphasis added).

Mr. McWhinney also testified that the data center has a point of presence for non-DOI customers and a separate point of presence for DOI customers, and that IDS are part of that configuration. He explained in credible detail that "we separated traffic from non-DOI customers from that of DOI customers. We separated the Internet access so it is a completely separate portal. Each one of these entities has their own series of firewalls, network intrusion detection sensors, and routers." Exh. 7 (Tr., Day 52 PM, pp. 36-37) (emphasis added); see Exh. 7 (Tr., Day 52 PM, p. 52). Mr. McWhinney also explained that, despite prior problems experienced by the Denver Data Center in implementing a program for the installation of host intrusion detection systems, the program has recently made significant headway, and steps have

been made to implement host intrusion detection systems not only at the NBC data center but also at other locations within the NBC. Exh.7 (Tr., Day 52 PM, pp. 40-41); see Exh. 8 (Tr., Day 53 AM, pp. 34-35).[6]

Plaintiffs' Notice completely ignores all of this unrefuted testimony. Plaintiffs were afforded the opportunity to call witnesses from the Department of the Interior or elsewhere to make their case during the 59-day hearing. Defendants even identified "Rule 30(b)(6)" witnesses whom Plaintiffs could examine for each relevant IT system, and Plaintiffs had the opportunity to cross-examine Defendants' witnesses at length. If any evidence supported the assertion that the NBC IT systems have no IDS – and we are aware of none – neither Defendants nor the Court deprived Plaintiffs of the opportunity to get it in the record.[7]

In the end, Plaintiffs' claim that NBC's systems lack IDS is based only upon their own misreading of the language of the September 2005 penetration report from ISS. In that report, ISS indicates that there were no indications of intrusion detection systems, and explains that none of the activities carried out against the NBC systems were blocked. September 2005 Technical Report, p. 21. However, the fact that ISS did not observe indications of IDS during

---

[6] Notably, Mr. McWhinney testified that when NBC migrates to the Enterprise Services Network ("ESN") in the near future, NBC is expected to keep all of its perimeter security in place and that, in addition, "the ESN does offer its own layer of security and its own layer of intrusion detection... ." Exh. 7 (Tr., Day 52 PM, p. 31-32). See Testimony of Stu Mitchell regarding this level of protection and its effectiveness. Exh. 9 (Tr., Day 43 AM pp. 49-51).

[7] For example, Plaintiffs cross-examined Mr. McWhinney. Despite their theory that NBC Denver lacks IDS, Plaintiffs' counsel never cross-examined Mr. McWhinney on whether it is true that NBC Denver has no IDS on its IT systems. Mr. Haycock, when asked by Plaintiffs' counsel whether there were IDS, replied that he believed there were. Exh. 6 (Tr., Day 49 PM, p.4, p.10, p. 13). The only testimony about the absence of IDS concerned a Boise LAN on a GSS separate from the Denver GSS. Exh. 6 (Tr., Day 49 PM, pp. 19-20; p. 62).

this particular penetration test does not, as Plaintiffs would have the Court believe, establish that NBC in fact has no IDS. It only means that none was detected during that time.[8] Indeed, ISS in its report acknowledged that NBC's system may have IDS by recommending to DOI that the existing security tools should be evaluated to determine if they are working effectively in the NBC environment, and that the vulnerabilities identified should be reviewed to determine if any monitoring or intrusion detection systems detected them appropriately. September 2005 Technical Report, p. 69. Similarly, on cross-examination, when Mr. Haycock was asked directly whether the fact that ISS was not detected in the NBC system in March, 2005, suggested that "there was no intrusion detection at that time," Mr. Haycock rejected that idea, stating "[i]t suggests that the intrusion detection didn't pick up his presence." Exh.6 (Tr., Day 49 PM, pp. 66-67). Mr. Haycock likewise denied that the failure to detect Mr. Brass' penetration meant that NBC's IDS was "ineffective":

> Q. Mr. Brass said he wasn't detected, and he testified under oath to that effect. That suggests there was no intrusion detection at that time, too, doesn't it?
>
> A. It suggests that the intrusion detection didn't pick up his presence.
>
> Q. So an ineffective intrusion detection, to the extent that it existed?
>
> A. I would not say that. I would say it depends on the method of his attack. He didn't even, as I understand it, attempt to penetrate our network, so the intrusion detection systems might not have picked that up.
>
> Q. He penetrated manually, didn't he?
>
> A. He gained access to databases through an application, as I understand.

---

[8] An IPS is a system that looks for anomalous or attack-type traffic and blocks it, while an IDS looks for the attack and then notifies an operator. Exh. 9 (Mitchell, Tr., Day 43 AM, pp. 44-45; see Exh. 9 (Tr., Day 43 AM at pp. 49-50). Therefore, the fact that ISS's penetration was not blocked does not preclude the existence of IDS within the NBC system.

Q. Manually, didn't he? Manually, correct?

A. Yes.

Exh. 6 (Tr., Day 49 PM, pp. 66-67). Mr. Brass's testimony supports Mr. Haycock's observations. Mr. Brass, the ISS penetration tester for NBC, testified that he designed his attack with the intent to avoid triggering the IDS in the NBC IT system:

> Not NBC. Other DOI branches, divisions, something. And I was aware that during his automated scanning he [Scott Miles] had often been detected by the divisions that he was assessing because they have these intrusion detection systems.
>
> So one of the first things I did after just doing sort of a by hand web based discovery process was ask my contact at the Inspector General's office, Roger Mahach, if he would like us to try to implement a more tell think [sic] [stealthy?] penetration that did not involve network scanning and that was solely conducted by hand, and his response was, yeah, that sounds great, let's do it. And that is the course of action that we pursued.
>
> So we didn't do a traditional test that would have given something -- you know, that would have had scan results for all of the hosts, and it was because I proposed a different style and they elected to see how that went.

Exh. 5 (Tr., Day 5 AM, pp. 19-20); Exh. 11 (Tr., Day 6 AM, pp. 8-9).

Plaintiffs' illogical leap to the conclusion that NBC has no IDS is completely refuted by the hearing record. Equally important, in light of the allegations made in Plaintiffs' Notice, the record provided a sound basis for Defendants' closing argument that the NBC IT system does have IDS.

III. Defendants Have Not "Waged A Campaign Of Slander Against The Inspector General"

Plaintiffs charge that Defendants, rather than remediating vulnerabilities in the DOI IT systems, have "waged a campaign of slander against the Inspector General... ." Notice at 4. This inflammatory charge is groundless. Although Plaintiffs cite the DOI Inspector General's

September 6, 2005 letter as support, the hearing record dispels this spurious allegation. For example, although the Inspector General's letter states that the Department and bureaus have been impugning the credentials and integrity of OIG staff and contractors, the Department's Chief Information Officer, Mr. Tipton, clearly did not. To the contrary, he was unequivocal in his favorable view of Roger Mahach, the person within OIG who managed the penetration testing efforts. Mr. Tipton testified that he has "the ultimate respect" for Mr. Mahach, described Mr. Mahach as a hard worker, and stated that, while he does not necessarily agree with Mr. Mahach's opinion, he respects it. Exh. 12 (Tr., Day 57 AM, pp. 74-76). Similarly, Associate Deputy Secretary Cason described his view of Mr. Mahach in this manner:

> In between, the IG managed to lure away the department's chief security officer, Roger Mahach, to the IG's office. So the person who knew the department the best in terms of where everybody was with IT security became the chief person for managing the penetration testing process. And that was okay with us. You know, it wasn't an issue for him to go.

Exh.13 (Tr., Day 50 AM, p. 52) (emphasis added).[9]

Plaintiffs have presented no hearing testimony from witnesses who attempted to undermine the credentials of the contractor, ISS. DOI employees generally acknowledged the expertise possessed by the contractor. Mr. Cason, for example, testified that he had no issue with ISS:

---

[9] Ironically, it was Plaintiffs who repeatedly attempted to impugn the integrity of Mr. Mahach during the course of the hearing. For example, they questioned his impartiality in performing his tasks for the OIG, Exh. 14 (Tr., Day 16 AM, pp. 73-78); see Exh. 15 (Tr., Day 21 AM, pp. 43-46), and strongly suggested to him that he violated his role as a Trusted Point of Contact and sabotaged the work of the Special Master by alerting members of DOI's IT staff to the Special Master's testing. Exh. 16 (Tr., Day 27 PM, pp. 66-94). Mr. Mahach made it plain that it was Plaintiffs and the publicizing of his testimony on a web site that made him feel that his integrity was under attack. Exh. 17 (Tr., Day 29 AM, pp. 2-6).

Q: Were you at all dissatisfied with the contractor, ISS, that the IG employed?

A: No. I had no reason to believe that there was any problem with ISS. And we explained to the IG's office that the fact that they were able to break in was fine. "Fine" is probably the wrong word. It was disappointing that they could, but that was their job, is to attempt to do that so that we could learn more about how our systems were configured in ways that might be exploitable. So the fact that they actually did the things that they were being paid to do was expected.

Exh.13 (Tr., Day 50 AM, pp. 57-58).

Plaintiffs quote from Defendants' closing argument as evidence of "the 'impugning [of] the credentials and integrity' of OIG staff." Notice at 4. This quotation serves only to demonstrate the fallacy of Plaintiffs' contention. The assertion within Defendants' closing argument that Roger Mahach and others from the OIG office were "without adequate current knowledge of the present state of IT security of any particular system" came directly from the testimony of Roger Mahach himself. On cross-examination, Mr. Mahach was simply asked whether, in light of the information he had in his possession about BIA, he could give a "competent and credible opinion about what the IT security posture is for BIA's systems today." Mr. Mahach responded, "I don't think I could, sir." Exh. 18 (Tr., Day 30 PM, pp. 33-34). When asked if he did not have enough information to give such an opinion, Mr. Mahach responded, "No, sir. I mean, at the system level, I don't." Exh. 18 (Tr., Day 30 PM, p. 34) Mr. Mahach was then asked whether anyone in the OIG had more information about non-OIG systems at Interior that he did, and he responded that they did not. Exh. 18 (Tr., Day 30 PM, pp. 40-42). Use of this testimony in Defendants' closing argument neither impugned Mr. Mahach's credentials nor called into question his integrity. In light of Mr. Mahach's own testimony, the claim of a

"campaign of slander" is indefensible.[10]

IV. The Hearing Record Establishes That The Department Of The Interior Responded To The Inspector General's Reports Of Penetration Testing Promptly, And Ordered Remediation To Address The Security Problems Noted

Plaintiffs characterize as "completely false" Defendants' assertions that the DOI responded appropriately to the IG's penetration test results, that the response was "prompt and measured," and that the DOI "ordered remediation to resolve the security problems noted." Notice at 3. Contrary to Plaintiffs' allegation, the hearing record fully supports these assertions in Defendants' closing argument. Thus, for example, Mr. Haycock testified that NBC developed an action plan immediately after NBC was informed of the penetration, and that many of the recommendations made to NBC by Mr. Brass "were completed almost immediately, within a few days after the penetration." Exh. 10 (Tr., Day 48 PM, pp. 67-68); see PX 33, Attachment 2. Significantly, Mr. Haycock testified specifically that NBC purchased Web Inspect and App Detective based upon Mr. Brass' recommendations, Exh. 10 (Tr., Day 48 PM, pp. 47-48), and Mr. Brass testified that App Detective was "a fine tool" that would very much help the database application security. Exh. 10 (Tr., Day 6 PM, p. 84). Thus, with the addition of App Detective, it is clear that NBC's IT security improved. Similarly, Mr. Haycock testified that Mr. Brass recommended "not show[ing] verbose error messages, because it tells the attacker exactly how to fix the problem." Exh. 10 (Tr., Day 48 PM, p. 68), and Mr. Brass testified that removing this error logging would "significantly" increase the security of the IT system. Exh. 11 (Tr., Day 6

[10] Similar testimony from Mr. Brass further supports Defendants' position. Mr. Brass testified that he could not make a statement about what NBC's security posture was as of May 9, 2005, because he had not examined NBC's IT system since the conclusion of his testing in April, 2005. Exh. 11 (Tr., Day 6 PM, p. 86).

PM, p. 82-83). Accordingly, NBC "turned off those error messages as he recommended." Exh. 10 (Tr., Day 48 PM, p. 68, Mr. Haycock testifying).[11]

Mr. Brass not only confirmed that the immediate steps taken by NBC significantly improved the security of NBC's system, he also established the cooperative nature of the DOI bureaus in addressing the problems observed as a result of the penetration testing, agreeing that the NBC technical staff was "very interested and very willing to implement the suggestions" he made. Exh. 11 (Tr., Day 6 PM, p. 79-80); see PX 651, p. 3 (in which the OIG observed that NBC indicated that the weaknesses identified in its IT system had been taken seriously and that NBC was acting to correct the deficiencies). Mr. Mahach similarly testified that DOI responded promptly to the IG penetration testing:

> Q: And NBC seems to have taken some considerable actions to remediate those vulnerabilities, haven't they?
>
> A: The NBC and BLM, at least – again, we haven't retested it so I can't speak technically. But in terms of their attentiveness and their response from their management down, yes, they were, I would say, engaged.

Exh. 18 (Tr., Day 30 PM, pp. 35-36) (Mr. Mahach acknowledged that BLM personnel were very concerned about the test results, and cooperative and eager to correct the vulnerabilities that were found).

Consistent with the above, Defendants asserted during closing argument that the NBC IT system "today is a lot more secure than when Mr. Brass saw it before. . . ." Plaintiffs impugn the

---

[11] Regarding BLM, Mr. James Rolfes similarly testified that, in response to the IG's penetration, BLM acted quickly to disconnect the public websites and disconnect Indian trust systems within the bureau. Exh.19 (Tr., Day 55 AM, p. 15). He also explained how BLM continued remediation efforts after the disconnections. Exh. 19 (Tr., Day 55 AM, pp. 21-29); DX 72.

character of Defendants' counsel and characterize this assertion as a "bald face lie." Notice at 8. Plaintiffs have no grounds for such a malicious allegation. As demonstrated through the testimony of Mr. Haycock and Mr. Brass, the record plainly supports the assertion that NBC's IT system is more secure than it was in March and April, 2005. Consistent with that testimony, Mr. Haycock further testified that NBC learned from the IG's penetration testing, and that NBC's immediate remediation efforts in response to it have made the NBC system more secure. Exh. 10 (Tr., Day 48 PM, pp. 66-70). He explained in detail the steps NBC carried out to remediate the vulnerabilities revealed by the testing, consistent with the action plan NBC developed. Id. Notably, Mr. Haycock testified, in addition to the actions described above, that:

> We have implemented a product called "Net Forensics," which is kind of an IDS repository that brings in all of the logging information that's collected on intrusion detection systems and off the servers themselves, so you can actually monitor automatically intrusion detection issues. That's been implemented on the DC LAN, and we're in the process of reviewing that for the Denver Data Center right now. That was another recommendation from the contractor.

Exh. 10 (Tr., Day 48 PM, p. 70).[12]

Mr. McWhinney also gave uncontroverted testimony on the remediation undertaken by NBC. He specifically noted that Mr. Brass had "indicated that there were a number of thing[s] that we could do immediately to improve our security posture," and then explained at length how NBC had taken the steps to accomplish those immediate tasks, thereby undeniably improving NBC's security posture. Exh. 7 (Tr., Day 52 PM, pp. 77-79); DX 61. In addition, Mr. Mahach

[12] This testimony further buttresses Defendants' representations that NBC systems contain IDS. Obviously, no need for an "IDS repository" would exist unless NBC systems used IDS in the first place.

likewise testified that he had received the report from NBC detailing the remediations that it had undertaken and that, if these were accomplished, the security status of NBC could be different than that witnessed by Mr. Brass in April, 2005. Exh. 18 (Tr., Day 30 PM, p. 35). This combined testimony from several witnesses supports Defendants' assertions at closing argument that the NBC IT system "today is a lot more secure than when Mr. Brass saw it before. . . ."

Notably, neither Mr. Haycock nor anyone else, including Defendants during closing argument, have contended that as a result of the remediation efforts in response to the IG reports, all of the IT security issues at NBC were forever and completely resolved or that the systems were perfectly secure. To the contrary, Mr. Haycock testified that remediation work was still ongoing as of mid-July, Exh. 10 (Tr., Day 48 PM, pp. 69-70), Exh. 6 (Tr., Day 49 PM, pp. 99-101), and that NBC's systems were not perfectly secure. Exh. 10 (Tr., Day 48 PM, p. 62). These facts, however, in no way undermine the evidence demonstrating that NBC's IT system is more secure than it was in April, 2005. Accordingly, Plaintiffs' rhetoric regarding this issue has no merit and deserves no further consideration by the Court.

V. Plaintiffs' Blatant Mischaracterization Of Defendant's Argument That The VPX Is Not A "Weak Link" Is Patently Unavailing, And The Record Clearly Supports Defendants' Argument Regarding The Security Of The VPX

Plaintiffs distort and blatantly mischaracterize Defendants' closing argument relating to the security of the VPX. Defendants' closing argument regarding the VPX did not attempt to rebut the truism that "interconnected systems are only as strong as their weakest link;" instead, Defendants rebutted Plaintiffs' fallacious assertion that the current VPX was the "weakest link" between the bureaus. To accomplish that, Defendants' closing argument did no more than recount the clear testimony of Stu Mitchell, the Department's system manager for the Enterprise

Services Network ("ESN").

Mr. Mitchell testified that, although there were "limited vulnerabilities" on the VPX as of June 2003, he did not consider the VPX connection to be a "weak link in the network security at Interior" at that time. He explained:

> [The 2003 version of the VPX was] a common connection point, and the weakness, if there is one, is that the firewall rules – that the security configurations were different between each bureau, but I wouldn't necessarily consider it a weak link.

Exh. 9 (Tr., Day 43 AM, pp. 33-35) (emphasis added). In addition, Mr. Mitchell explained that the VPX connection that existed in 2003 had been modified, with the inclusion of additional firewalls: "The department now has installed firewalls in between the VPX routers and the bureau firewalls, and there is an addition of a VBNS, an MCI wide-area network circuit, that taps into an Intranet cloud, or an Intranet whiting." Exh. 9 (Tr., Day 43 AM, p. 36). Those additional departmental firewalls that have been added to the VPX connection are controlled by ESN, over which Mr. Mitchell serves as the system manager. Exh. 9. (Tr., Day 43 AM, p. 37).

Plaintiffs' cross-examination of Mr. Mitchell elicited even more testimony from Mr. Mitchell establishing the security of the VPX:

> Q: Is it your understanding that the VPX adds security to the systems or perimeter security of the bureaus?
>
> A. Yes. You have to -- some people think of perimeter security as a security that connects the bureaus to the Internet. It adds to perimeter security where the bureaus connect to each other.
>
> Q: So the answer to my question is yes, it does provide security. Correct?
>
> A. Yes, it provides security. . . . Excuse me. I need to make sure that we're talking about the VPX as it stands today, because that's the

one that has the firewall rules. And if you talk about the VPX as it was back in June 2003, each bureau was responsible for providing the security that connected to the VPX. And the VPX was essentially nothing more than a set of routers that connected those bureau networks together.

* * *

Q: And an enhanced VPX, is that being replaced by ESN?

A: The ESN intranet, yes. It will be folded into the ESN.

Q: So let's just make sure we have this clear. In 2003 you had a VPX, right?

A: Right, uh-huh.

Q: And in the beginning of 2005 you had an enhanced VPX. Correct?

A: Yes.

Q: And an enhanced VPX that was actually provided interim authority to operate, correct, in the beginning of 2005. Correct?

A: That's correct.

Q: Okay. So today we have ESN, but it hasn't replaced the enhanced VPX yet, has it?

A: Yes. Actually, what we did was, with the ATO [,] is we rolled in the VPX as the ESN intranet, and we're expanding the VPX to fill part of the ESN intranet role.

Q: . . . . But you have incorporated, then, the enhanced VPX into the developing ESN. Correct?

A: Yes.

Exh. 20 (Tr., Day 43 PM, p. 9, pp. 22-23) (emphasis added).

In light of the fact that Defendants' closing argument repeated almost verbatim the uncontradicted testimony of Mr. Mitchell, Plaintiffs' characterization of this portion of the closing as a "gross distortion" is extremely ill-conceived. There is simply no basis for such an allegation.[13] Accordingly, the Court should dismiss those allegations as unfounded.

VI. The Hearing Record Contains No Evidence That Any Unauthorized Access Resulted In Malicious Alteration Or Damage To Individual Indian Trust Data

Plaintiffs chastise Defendants for asserting at closing that "there is no evidence that there has been any unauthorized access that maliciously altered or damaged individual Indian trust data on the system." Notice, p. 7. Plaintiffs allege that this assertion is "absurd" because "the absence of intrusion detection systems and audit logs ensures that no evidence can exist." Id. However, as demonstrated above, the factual premise of Plaintiffs' allegation is wrong. Unrefuted evidence and testimony establish the existence of IDS within NBC. The use of IDS in other DOI bureaus has also been established. E.g., Exh. 21 (Tr., Day 46 AM, pp. 56-57), Exh. 21 (Tr., Day 46 PM, p. 65) (MMS employs IDS); Exh. 22 (Tr., Day 32 PM, p. 103), Exh. 22 (Day 35 AM, p. 59, Brian Burns testifying) (BIA employs IDS). Moreover, Plaintiffs have not demonstrated that the bureaus do not possess audit logs. To the contrary, the testimony shows that, while there may have been issues regarding the effectiveness of these logs, the logs do exist and are reviewed. See Exh. 7 (Tr., Day 52 PM, pp. 35, 46-47, 64, 82-83).

Finally, although Plaintiffs note that the Inspector General's contractor did not attempt to manipulate or alter Trust data, they overlook the fact that the IG's testing was requested by DOI

[13] Moreover, while Plaintiffs quote the Inspector General's memorandum, that quoted language does not even address the current VPX or the ESN, and does not justify their allegations in the least.

itself and could not equate to malicious hacking or alteration of data by a hacker. DOI's own initiatives to improve IT security cannot serve as evidence of a malicious hacker. Such testing is not unauthorized and helps DOI identify vulnerabilities and address them before malicious hackers can find and exploit them. In sum, despite 59 days of hearing testimony, Plaintiffs failed to provide evidence demonstrating that individual Indian trust data had been maliciously altered or damaged as a result of unauthorized access.

VII. Conclusion

In light of the evidence and hearing testimony set forth above, the Court should reject the allegations Plaintiffs make concerning Defendants' closing argument and summarily dismiss those allegations as meritless.

Dated: October 14, 2005

Respectfully submitted,

ROBERT McCALLUM, JR.
Associate Attorney General
PETER D. KEISLER
Assistant Attorney General
STUART E. SCHIFFER
Deputy Assistant Attorney General
J. CHRISTOPHER KOHN
Director

/s/ Robert E. Kirschman, Jr.
ROBERT E. KIRSCHMAN, JR.
(D.C. Bar No. 406635)
Assistant Director
GLENN D. GILLETT
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 307-0494
Facsimile: (202) 514-7162

CERTIFICATE OF SERVICE

I hereby certify that, on October 14, 2005 the foregoing *Defendants' Response to Plaintiffs' Notice of Supplemental Information in Support of Plaintiffs' Motion for Information Technology Security Preliminary Injunction* was served by Electronic Case Filing, and on the following who is not registered for Electronic Case Filing, by facsimile:

Earl Old Person (*Pro se*)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
Fax (406) 338-7530

/s/ Kevin P. Kingston
Kevin P. Kingston